RSAC 2025 Conference

Many Voices.
One Community.

SESSION ID: GRC-T10

It's Always Risky in IT: Frontline Stories and Strategic Insights

Rohit Bansal

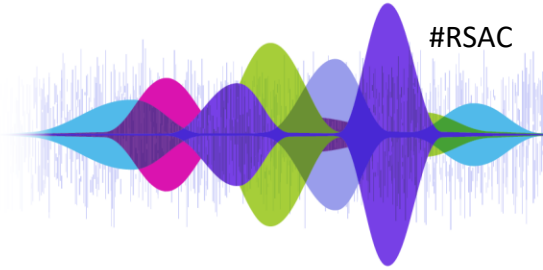
Security Engineer
Grammarly
LinkedIn

Gourav Nagar

Director - Information Security
Bill.com
Linkedin

The Balance: Productivity vs Security

Who are we?



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

Real World Case Studies

Risk reduction in high-velocity companies

- Shadow IT Apps – Protecting the company from the usage of un-sanctioned apps and accounts
  - Company data in free accounts used by business
    - Cloud Storage tools
    - Documentation/Transcription tools
    - Email productivity tools
  - Cost of procurement and various reviews
  - Productivity loss by blocking the usage

Risk reduction in regulated companies

- Zero Trust – Protect usage of sensitive company resources through trusted channels of identity, device, and business need.
  - Network restrictions for sensitive company systems
    - Customer Support Tools
    - Build and Development tools
- Businesses need to know the requirements
- Known device and Device posture requirements
- Traditional VPNs provide all or no solution

Common Issues faced

- Complexity
- Cost and Resource Strain
- Legacy System Integration
- Operational Challenges and User Experience
- Cultural and Organizational Resistance
- Scalability and Performance
- Data and Identity Management
- Interoperability and Compatibility

over
Ave
MORRIS
650
COUNTY

RSAC 2025 Conference

Introducing Framework: D.A.C.I.M.I.

Many Voices.
One Community.

Discovery

- Risk Register
- Risk Prioritization
- Definition of Outcome
- Success criteria
- Out of Scope
- Residual Risk Assessment

Alignment

- Cost
- Build vs Buy
- Proof of Value
- Integration with other systems
- Stakeholders
- Customer Experience
- X-Functional Partners
- Impact of unknown

Communication

- Socialize rationale
- Engage champions through opt-in
- Early feedback opportunities
- Recovery from failures
- Continuity of messages
- Multiple channels

Implementation

- Choice of implementation
  - Seek early wins vs Existing use cases
  - Fall back vs Roll back
- Choice of initial user population
  - Vocal vs adaptable customers
  - At risk vs less risky customers
- Choice of user engagement
  - Integrated vs New interface

Implementation

- Choice of ambiguity
  - Knowing all answers vs path of experimentation
- Choice of execution speed
  - Fast vs Gradual
- Choice of replacement
  - Easy vs Hard to replace in future
- Choice of maintainability or training

Maturity

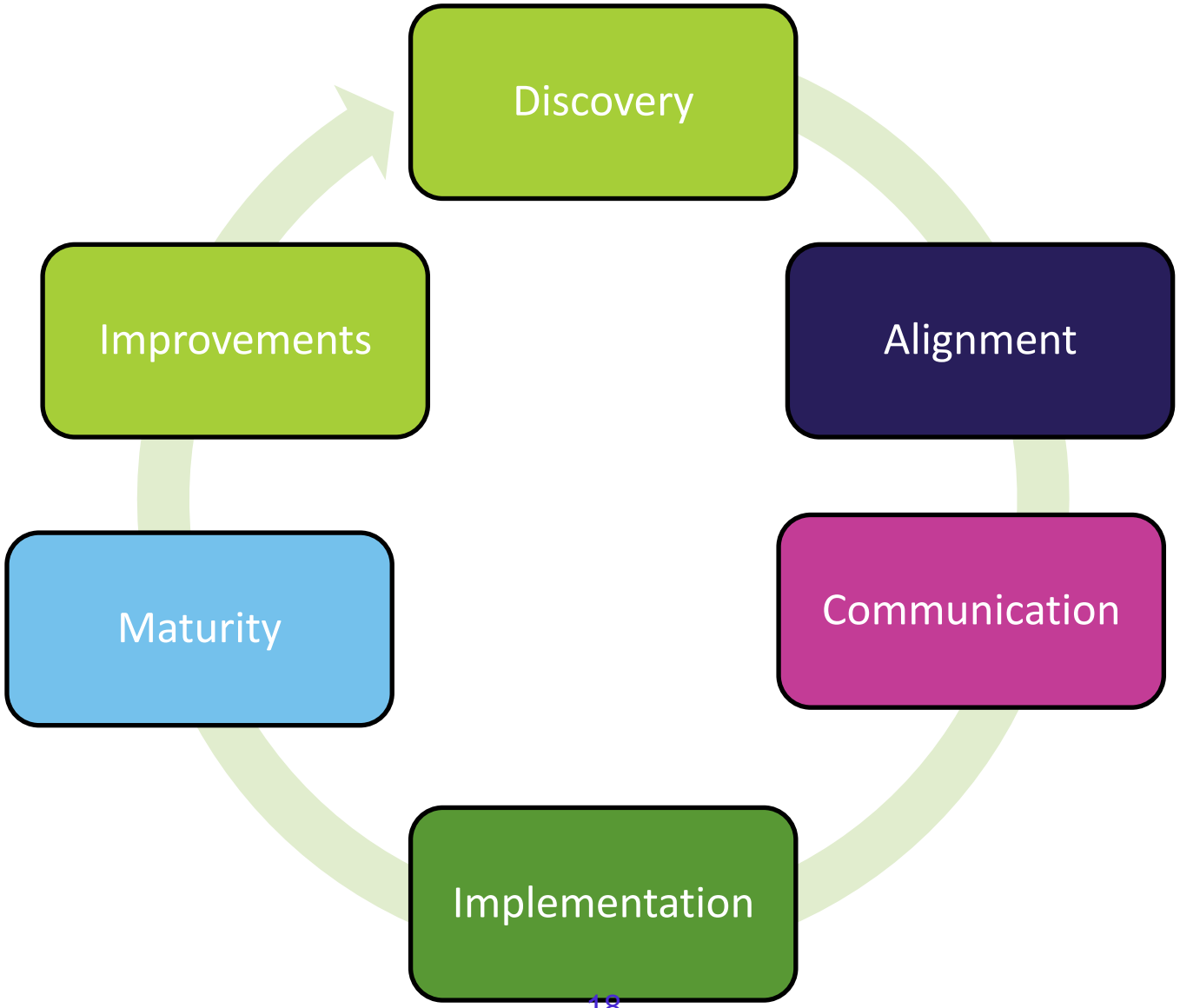
- Documentation
- Active monitoring
- KPI and Metrics
- Team re-composition

!! Automate, Automate, Automate !!

Improvements

- Evolving needs of business
- Fresh perspectives
- Change in scope
- Keep up with innovation
- Risk revaluation

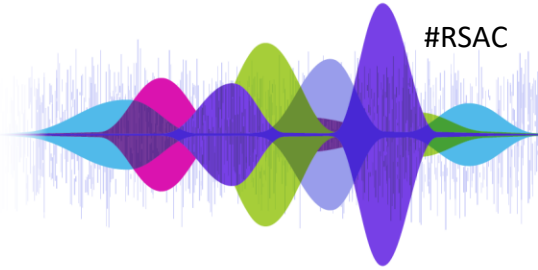
Framework: D.A.C.I.M.I



Benefits

- High Chances of a Successful Project!
- Cross functional Relationships
- Time Savings
- Cost Savings
- Better Security for your company

Next Steps



- Next week...
  - Look at unmitigated risks
- In the first three months...
  - Complete Discovery and Alignment exercises for one risk area
- Within six months...
  - Complete the Implementation the chosen risk area
  - Establish the Maturity model (replace the initial team)
  - Look at future improvements or move to another risk

RSAC™ | 2025 Conference

Many Voices.
One Community.